# OSINT Report on Innovatech Solutions

## Summary

This report outlines the data gathered from job postings by Innovatech Solutions, a cybersecurity firm focused on industrial cybersecurity and critical infrastructure protection. The data provides insights into the company's structure, technologies used, work practices, and other aspects that could be of use in a penetration test or social engineering attack.

## Details

The job postings by Innovatech Solutions reveal the following:

1. \*\*Company Location\*\*: Innovatech Solutions is located in Novatech City, United States.

2. \*\*Company Size and Structure\*\*: The company seems to be a sizable organization with multiple departments, including Engineering, Product Management, and Legal.

3. \*\*Technologies Used\*\*: They use Rust programming language and Linux systems. They also utilize RabbitMQ or similar messaging systems.

4. \*\*Software Development Practices\*\*: They follow agile development practices and use a microservice system architecture.

5. \*\*Customer Support Operations\*\*: They use a ticket-based workflow for customer support, specifically Zendesk or something similar.

6. \*\*Operational Technology (OT)\*\*: The company is involved in sectors like industrial control systems, manufacturing, or utility services.

7. \*\*Diversity and Inclusion\*\*: The company is committed to diversity and inclusion, suggesting a multicultural and diverse workforce.

8. \*\*Compensation Structure\*\*: The company offers an equity-based compensation package, suggesting it may be privately held or have a share scheme for employees.

## Significant Findings

1. \*\*Technologies Used\*\*: The use of Rust, Linux, and RabbitMQ can provide a focus on looking for known vulnerabilities in these systems during the penetration test.

2. \*\*Software Development Practices\*\*: The agile development practices and microservice system architecture could indicate potential areas of complexity and thus potential weaknesses in their system.

3. \*\*Workforce Diversity\*\*: The diverse and multicultural workforce could be leveraged in social engineering attacks.

4. \*\*Company Expansion\*\*: The focus on recruitment and equity-based compensation indicates the company is in a growth phase, which might make them vulnerable to social engineering attacks targeted at new or less experienced employees.

## Recommended Follow-up Actions

1. \*\*Technology Exploration\*\*: Research known vulnerabilities related to Rust, Linux, RabbitMQ, and microservices to identify potential weak points in the system.

2. \*\*Employee Profiling\*\*: Use social networks to identify employees, especially new hires or less experienced staff, for potential social engineering attacks.

3. \*\*Company Structure Analysis\*\*: Understand the company's structure and departments to find potential areas of weakness.

4. \*\*Further OSINT\*\*: Conduct further OSINT on the company's operations, their security measures, and potential vulnerabilities in their infrastructure.